

AFFIDAVIT

I, Terrance L. Taylor, being duly sworn, do hereby depose and state the following:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I have been so employed with HSI since March 2012. I am currently assigned to the Office of the Resident Agent in Charge, HSI Charleston, West Virginia (WV). Since this time, I have gained experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

2. I am a Special Agent with twenty years of federal law enforcement experience. Prior to my employment with HSI, I was a Police Officer for two years in Huntington, WV, a Special Agent with the United States Department of State-Bureau of Diplomatic Security for six years, a Special Agent with the Naval Criminal Investigative Service for two years, and a Special Agent with the United States Department of State-Office of Inspector General for two years. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Center (“FLETC”) and a graduate of the West Virginia State Police Academy. I graduated from the Criminal Investigator Training Program in 2002, and the Immigration and Customs Enforcement Special Agent Training Program in 2012. As part of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. These areas include laws and regulations pertaining to the importation of various types of merchandise and

contraband, prohibited items, money laundering, and various immigration violations. I have more specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, 2256 and 2422.

3. As a Special Agent, I have investigated federal criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training at the FLETC, Immigration and Customs Enforcement, as well as everyday work relating to investigations involving the receipt, possession, access with intent to view, production, importation, advertising, and distribution of child pornography that occur in the Northern District of West Virginia. I have received training in the areas of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have obtained search warrants for child pornography offenses, and I have been the case agent or assisted others in numerous investigations involving the sexual exploitation of children. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by law to request a search warrant.

4. I make this Affidavit in support of an application for a search warrant to conduct a search of Carl Dennis COLVIN's property (SUBJECT PROPERTY) in HSI's custody in Charleston, West Virginia, which was previously seized pursuant to a State of West Virginia search warrant. A written description of the SUBJECT PROPERTY is set forth in Attachment A and incorporated herein. I am investigating COLVIN for violations of Title 18 U.S.C. §§

2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography). With the SUBJECT PROPERTY I seek to search for evidence and instrumentalities of criminal violations set forth above for items specified in Attachment B, incorporated herein by reference, which may be found, and to search all items listed in Attachment B as instrumentalities and evidence of a crime.

5. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts necessary to establish probable cause that evidence and instrumentalities of a violations of Title 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography), are presently located within the SUBJECT PROPERTY.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

STATUTORY AUTHORITY

7. The investigation concerns violations of Title 18, United States Code, Sections 2252A(a)(2) and 2252A(a)(5)(B), relating to matters involving the sexual exploitation of minors.

a) 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving

or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

- b) 18 U.S.C. § 2252A(a)(5)(B) prohibits any person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

- 8. The following definitions apply to this Affidavit and its Attachments.
 - a) The term “**minor**,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.
 - b) The term “**child erotica**” means materials or items that are sexually arousing to persons having a sexual interest but that are not necessarily in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
 - c) The term “**child pornography**,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable form, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
 - d) The term “**sexually explicit conduct**,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

- e) The term “**visual depiction**,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- f) The term “**computer**,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- g) The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact disks, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
- h) “**Internet Service Providers**” (“**ISPs**”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co- locations of computers and other communications equipment.
- i) “**Internet Protocol address**” (“**IP address**”), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet.

IP addresses might also be static if an ISP assigns a user's computer a particular IP address each time the computer accesses the Internet.

- j) **"Websites"** consist of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").
- k) **"Chat,"** as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.
- l) **"Cloud-based storage service,"** as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.
- m) **"Computer hardware,"** as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- n) **"Computer software,"** as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- o) **“Computer passwords and data security devices,”** as used herein, consist of information designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.
- p) **“Mobile applications,”** as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.
- q) **“Peer to Peer File Sharing” (“P2P”)** is a free open source software process that allows computer users, utilizing the same file sharing software, to connect to each other and directly access files from one another’s computer hard drive. The files to be shared with others across the Internet are selected as shareable by each individual computer user. This action is usually done by the computer user who will place files he/she wishes to share into a specific folder often times titled “Shared Folder”. The software only allows remote users to access this “shared folder” and thus prevents access to the rest of the computer hard drives contents. Some examples of peer to peer files sharing software are Napster, Kazaa, Grokster, Gnutella, eMule, Morpheus, Phex, Ares, BitTorrent, etc.
- r) **“Remote Computing Service” (“RCS”)**, as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS,
THE INTERNET, AND EMAIL**

9. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

10. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced

using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skill were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

11. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

12. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through FTPs to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution

and receipt of child pornographic materials among pornographers.

13. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and other electronic devices such as cell phones or even gaming consoles has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

14. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

15. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc., and Google, Inc., among others. The online services allow a user to set up an account with a remote. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

**SPECIFICS OF SEARCHES OF COMPUTER
AND ELECTRONIC DEVICE SYSTEMS**

16. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

17. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on the computer indefinitely until overwritten by other data.

18. As described further in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PROPERTY, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B), of any electronic device previously seized from COLVIN and currently in HSI's custody.

19. I submit that the electronic devices previously seized from COLVIN are believed to contain records referenced above to be stored on those electronic devices, for at least the following reasons:

- a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months

or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b) Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- d) Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- e) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

20. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium on the SUBJECT PROPERTY because:

- a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b) Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner.
- d) Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.
- e) Some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user.

- f) Moreover, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- g) A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h) The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- i) Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- j) I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

21. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit searching, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and its attachments, and would authorize a review of the media or information consistent with the warrant. The review may

require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

22. Based upon my knowledge, experience, and training in criminal investigations, particularly those that focus on child exploitation, as well as the training and experience of other law enforcement officers trained in child exploitation and child pornography investigations with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

- a) Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b) Collectors of child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce or to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c) Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d) Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.
- e) Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of

time even after the individual “deleted” it.¹

- f) Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- g) Collectors of child pornography prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes. These materials are often kept on their person in forms of media storage devices such as thumb drives and cellphones in their pants pockets and on their keychains.
- h) Further, it is common for such users to save and transfer the pornographic images and/or pornographic video of children from one computer to another because the images are generally difficult to obtain securely.

23. Your Affiant believes that given the continuing nature of possession of child pornography and the general character of such offenders as “collectors” and “hoarders,” there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B)

¹ See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

(possession of child pornography) will be present on the SUBJECT PROPERTY as described in Attachment A, when the search is conducted.

PROBABLE CAUSE

24. On July 6, 2022, Wheeling Police Department (WPD) officers were dispatched to the area of Cecil Street and Lumber Avenue, Wheeling, Ohio County, West Virginia, regarding a verbal domestic dispute between a father and son. WPD officers subsequently identified the two individuals as Sean Lee Colvin (son) and Carl Dennis COLVIN (father). Sean advised that he and his father got into an argument about people Sean associates with. Sean further advised that the argument was also about possession of child pornography that COLVIN had on his cellphone.

25. Sean stated he had had the last straw with his father attacking him and took COLVIN's cellphone from him and began to look through it. Sean further stated that the cellphone accounts was in his name and that he did not want to get in trouble for the stuff on his father's cellphone. Sean advised when he unlocked COLVIN's cellphone he saw a photograph of children naked. WPD officers subsequently spoke with COLVIN, who then advised he did not know what officers were talking about. COLVIN further advised he was arguing with his son about who Sean hangs out with.

26. WPD officers notified HSI Task Force Officer (TFO), WPD Detective, William Castilow regarding the incident. TFO Castilow subsequently obtained a State of West Virginia search warrant to search COLVIN's cellphone for violations of child exploitation. TFO Castilow provided the search warrant to COLVIN and subsequently seized COLVIN's cellphone.

27. TFO Castilow issued COLVIN his Miranda Warnings. COLVIN waived his

Miranda Warnings and voluntarily agreed to be interviewed. During the interview TFO Castilow asked COLVIN questions about child pornography on his cellphone. COLVIN stated that unknown individuals sent him all kinds of different images to include child pornography and that he did not conduct searches of his own to find images of child pornography. COLVIN further stated that over 100 images of child pornography would be found on his cellphone.

28. TFO Castilow subsequently obtained a State of West Virginia search warrant to search and seize evidence at COLVIN's residence located at 2357 Overbrook Avenue, Apartment #4, Wheeling, Ohio County, West Virginia. TFO Castilow seized numerous electronic devices that include the SUBJECT PROPERTY.

29. During a preliminary computer forensic review of COLVIN's cellphone, TFO Castilow identified over 600 images of child pornography to include images of bestiality. COLVIN was arrested on State of West Virginia violations for possession of child pornography on August 22, 2022.


CONCLUSION

30. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the locations described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PROPERTY described in Attachment A, authorizing the search of the items described in Attachment B.

31. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in

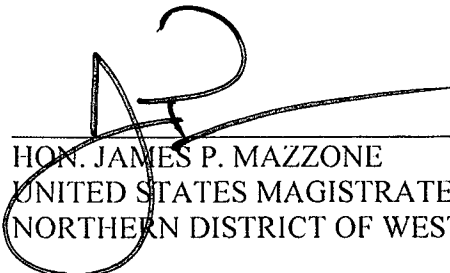
a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the electronic devices. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.



SPECIAL AGENT TERRANCE L. TAYLOR
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this
6th day of July, 2023.



HON. JAMES P. MAZZONE
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF WEST VIRGINIA